

La consulta plantea dudas sobre la adecuación a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal en la instalación de un sistema de videovigilancia embarcada en los autobuses que prestan servicio de transporte público de viajeros y un sistema de videovigilancia en los frontales de los autobuses

Según señalan, el sistema de cámaras embarcadas, captaría la imagen del conductor para identificar posibles conductas o comportamientos que pongan en riesgo la seguridad de las operaciones con la finalidad de prevenir accidentes por causas imputables al personal de conducción.

Por otro lado, el sistema de cámaras frontales, tendrían como finalidad la prevención e investigación de accidentes y captaría imágenes de la vía pública por la que circula el autobús.

Se plantea por tanto la legitimación y medidas a implantar para la adecuación a la ley 15/1999 legalidad de un sistema de videovigilancia en el que el fin último de la medida propuesta, si bien expresada en términos muy generales, sería la de reducir accidentes y proteger la integridad física de las personas que usan los servicios de transporte por carretera.

Planteada así la cuestión, procede su análisis de manera diferenciada, en cuanto a las cámaras a instalar en el interior de los vehículos por un lado, y por otro aquellas cámaras que se instalarán en el frontal y que captan la vía pública. Comenzaremos estudiando la cuestión que afecta a las cámaras en el interior de los vehículos, cuestión que puede afectar de una manera importante al control de los trabajadores.

I

En primer lugar, los sistemas de videovigilancia suponen un tratamiento de datos de carácter personal, de conformidad con los artículos 1 y 2.1 Ley



15/1999. La normativa que nos ocupa tiene por objeto la protección de los datos de carácter personal como derecho fundamental, definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la Ley, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*. El Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en su artículo 5.1.f) precisa que constituye un dato de carácter personal *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.”*

Por su parte, el artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”*. De acuerdo con esta definición de tratamiento de datos personales, la captación y en su caso grabación de imágenes de las personas constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada.

En este mismo sentido se pronuncia la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

Partiendo de este principio general, la vigilancia por videocámaras puede estar justificada en determinadas circunstancias, sin embargo se hace necesario adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos de manera que el tratamiento de imágenes con fines de videovigilancia sea adecuado a los principios de la Ley Orgánica 15/1999 y garantizar así los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.

A este respecto la citada Instrucción 1/2006, remite en su artículo 2 a lo previsto en el artículo 6.1 y 2 de la Ley Orgánica 15/1999, donde se establece que *“el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”*, sin perjuicio de que dicho consentimiento podrá quedar excluido, de acuerdo con lo dispuesto por el artículo 6.2 cuando, el tratamiento sea necesario para el



adecuado desenvolvimiento de la relación laboral de los trabajadores con la empresa.

El artículo 20.3 del Texto Refundido del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015 de 23 de octubre – cuyo tenor literal apenas ha cambiado respecto de la versión anterior en lo que ahora interesa – , dispone que *“El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad”*.

En este sentido, el artículo 20.3 del Estatuto de los Trabajadores en relación con el art. 6.2 de la Ley 15/1999 legitimaría, en principio, a la consultante como empleadora para tratar las imágenes de los trabajadores en el ámbito laboral con carácter general.

Y así lo ha venido reiterando la jurisprudencia en lo que a empleados públicos se refiere amparado en el art. 6.2 Ley 15/1999, como en Sentencia de la Sala Tercera del Tribunal Supremo de 2 de julio de 2007 (Rec. 5017/2003) que señala que el control del cumplimiento del horario de trabajo a que vienen obligados los empleados públicos es inherente a la relación que une a estos con la Administración en cuestión, y no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos. Asimismo, la Sentencia de la misma Sala de 2 de julio de 2007 (Rec. 5017/2003) indica: *“Desde luego, la finalidad perseguida mediante su utilización es plenamente legítima: el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos. Y, en tanto esa obligación es inherente a la relación que une a estos con la Administración Autonómica, no es necesario obtener previamente su consentimiento ya que el artículo 6.2 de la Ley Orgánica 15/1999 lo excluye en estos casos”*.

Ahora bien, esta legitimación no es absoluta y exige que el empresario informe de dicho tratamiento a los trabajadores (cumpliendo así con el deber de informar previsto tanto en el artículo 10 de la Directiva 95/46/CE como en el artículo 5 de la Ley 15/1999). Y no sólo a los trabajadores, sino también a sus representantes. En este punto resulta ilustrativa y capital la Sentencia del Tribunal Constitucional 29/2013, de 11 de febrero, recurso de amparo 10522/2009, cuya conclusión es: *“Por tanto, no será suficiente que el*



tratamiento de datos resulte en principio lícito, por estar amparado por la Ley (arts. 6.2 LOPD y 20 LET), o que pueda resultar eventualmente, en el caso concreto de que se trate, proporcionado al fin perseguido; el control empresarial por esa vía, antes bien, aunque podrá producirse, deberá asegurar también la debida información previa (...) No contrarresta esa conclusión que existieran distintivos anunciando la instalación de cámaras y captación de imágenes en el recinto universitario, ni que se hubiera notificado la creación del fichero a la Agencia Española de Protección de Datos; era necesaria además la información previa y expresa, precisa, clara e inequívoca a los trabajadores de la finalidad de control de la actividad laboral a la que esa captación podía ser dirigida. Una información que debía concretar las características y el alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo”.

En este sentido hay que tener en cuenta la Sentencia de la Sala de lo Social del Tribunal Supremo de 13 de mayo de 2014, rec. 1685/2013 en un supuesto de despido de una trabajadora derivado de incumplimientos a través de las imágenes captadas por un sistema de videovigilancia, que dispone lo siguiente: *“por la empresa no se dio información previa a la trabajadora de la posibilidad de tal tipo de grabación ni de la finalidad de dichas cámaras instaladas permanentemente, ni, lo que resultaría más trascendente, tampoco se informó, con carácter previo ni posterior a la instalación, a la representación de los trabajadores de las características y alcance del tratamiento de datos que iba a realizarse, esto es, en qué casos las grabaciones podían ser examinadas, durante cuánto tiempo y con qué propósitos, ni explicitando muy particularmente que podían utilizarse para la imposición de sanciones disciplinarias por incumplimientos del contrato de trabajo”*

Y así ha venido aplicándose por esta Agencia, como en la Resolución recaída en el PS/00724/2014. En definitiva, el tratamiento de imágenes de los trabajadores con fines de control laboral está admitido con carácter general, al aparecer legitimado por el art. 20.3 del Estatuto de los Trabajadores, en la medida en que cumpla todos los requisitos de la Ley 15/1999 incluyendo en todo caso la previa información a los trabajadores y a sus representantes.

Sin embargo, recientemente la Sentencia del Pleno del Tribunal Constitucional de 3 marzo 2016, recurso de amparo 7222/2013 ha modulado las afirmaciones anteriores, al indicar que el sistema de videovigilancia con fines de control laboral, al aparecer amparado en el art. 20.3 ET en relación con el art. 6.2 LOPD, no requiere del consentimiento del trabajador, pero además el deber de información al trabajador puede entenderse cumplimentado con la utilización de los genéricos distintivos informativos en lugar suficientemente visible y teniendo a disposición de los interesados impresos en los que se detalle la información prevista en el art. 5. Señala la citada sentencia:

“Aplicando la doctrina expuesta al tratamiento de datos obtenidos por la instalación de cámaras de videovigilancia en el lugar de trabajo, que es el problema planteado en el presente recurso de amparo, debemos concluir que el empresario no necesita el consentimiento expreso del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 TRLET , que establece que “el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana”. Si la dispensa del consentimiento prevista en el art. 6 LOPD se refiere a los datos necesarios para el mantenimiento y el cumplimiento de la relación laboral, la excepción abarca sin duda el tratamiento de datos personales obtenidos por el empresario para velar por el cumplimiento de las obligaciones derivadas del contrato de trabajo. El consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario.

En definitiva, la exigencia de finalidad legítima en el tratamiento de datos prevista en el art. 4.1 LOPD viene dada, en el ámbito de la videovigilancia laboral, por las facultades de control empresarial que reconoce el art. 20.3 TRLET, siempre que esas facultades se ejerzan dentro de su ámbito legal y no lesionen los derechos fundamentales del trabajador”.

Incide sin embargo dicha resolución en la necesaria observancia del principio de proporcionalidad: *“Por ello, como hemos señalado, aunque no se requiere el consentimiento expreso de los trabajadores para adoptar esta medida de vigilancia que implica el tratamiento de datos, persiste el deber de*



información del art. 5 LOPD. Sin perjuicio de las eventuales sanciones legales que pudieran derivar, para que el incumplimiento de este deber por parte del empresario implique una vulneración del art. 18.4 CE exige valorar la observancia o no del principio de proporcionalidad. Debe ponderarse así el derecho a la protección de datos y las eventuales limitaciones al mismo justificadas en el cumplimiento de las obligaciones laborales y las correlativas facultades empresariales de vigilancia y control reconocidas en el art. 20.3 TRLET, en conexión con los arts. 33 y 38 CE. En efecto, la relevancia constitucional de la ausencia o deficiencia de información en los supuestos de videovigilancia laboral exige la consiguiente ponderación en cada caso de los derechos y bienes constitucionales en conflicto; a saber, por un lado, el derecho a la protección de datos del trabajador y, por otro, el poder de dirección empresarial imprescindible para la buena marcha de la organización productiva, que es reflejo de los derechos constitucionales reconocidos en los arts. 33 y 38 CE y que, como se ha visto, en lo que ahora interesa se concreta en la previsión legal ex art. 20.3 TRLET que expresamente faculta al empresario a adoptar medidas de vigilancia y control para verificar el cumplimiento por los trabajadores de sus obligaciones laborales (STC 186/2000, de 10 de julio, FJ 5; 170/2013, de 7 de octubre, FJ 3). Esta facultad general de control prevista en la ley legitima el control empresarial del cumplimiento por los trabajadores de sus tareas profesionales (STC 170/2013, de 7 de octubre; STEDH de 12 de enero de 2016, caso Barbulescu v. Rumania), sin perjuicio de que serán las circunstancias de cada caso las que finalmente determinen si dicha fiscalización llevada a cabo por la empresa ha generado o no la vulneración del derecho fundamental en juego”.

Ahora bien, esto no implica que en el ámbito laboral quepa todo tratamiento de datos personales para el control por el empresario del cumplimiento de los deberes laborales del trabajador, puesto que habrá de observarse el principio de proporcionalidad consagrado en el art. 4.1 LOPD únicamente permitiendo el tratamiento de datos “adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido”.

Respecto de la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de “una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad,

y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.

En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)».

Por consiguiente, cualquier medida de control que se adopte debe superar este juicio de proporcionalidad, determinando si la medida es adecuada, necesaria y equilibrada, ya que en otro caso resulta desproporcionada y por ello contraria a la normativa de protección de datos.

En definitiva, el control laboral como causa legitimadora para el tratamiento de datos personales no implica, que quepa todo tratamiento de datos amparado en dicha finalidad. En el informe 475/2014 disponible en nuestra página web contemplábamos una serie de criterios, extraídos tanto de informes del Grupo de Berlín, como del Grupo de Trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; en particular en su Dictamen 8/2001 (WP 48), sobre el tratamiento de datos personales en el contexto laboral, así como en el Documento de Trabajo de 29 de mayo de 2002 (WP 55), relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo en el que se examina la vigilancia por el empleador de la utilización del correo electrónico e Internet por parte de los trabajadores; y finalmente de la Recomendación CM/Rec (2015) 5 del Comité de Ministros del Consejo de Europa de 1 de abril de 2015 sobre el tratamiento de datos en el ámbito laboral.

Con carácter general, esta Agencia entiende que si bien cabe la captación de imágenes de los trabajadores con fines de control laboral, ello no puede realizarse de modo que suponga una monitorización constante y completa de los trabajadores. De este modo, si bien cabe la captación de imágenes en el lugar de efectiva prestación de servicios por el empleado, excluyendo los lugares no destinados a tal fin, como vestuarios u habitaciones, comedores o lugares de descanso, la finalidad ha de ser el control por el empresario en el lugar de trabajo, pero no cabe una monitorización del trabajador durante toda su jornada en el lugar de trabajo que supondría una medida intrusiva y probablemente desproporcionada en relación con la finalidad perseguida, sin ser una respuesta proporcionada ante riesgos potenciales o concretos.

En conclusión, no cabe la instalación de un sistema de videovigilancia que, con carácter permanente y no discriminando situaciones concretas, implicara la captación y grabación de las imágenes de los trabajadores en el interior de los vehículos. Otra cosa sería que el sistema se implantara específicamente en determinados momentos o casos en que pudiera plantearse un presunto incumplimiento concreto y particular de un determinado trabajador o grupo de trabajadores; o bien que el sistema se concibiera de tal modo que sólo se activara la grabación ante determinados eventos, como puede ser un posible accidente de circulación, o en determinados casos.

II

En segundo lugar, se plantea la cuestión relativa a la implantación de sistema de cámaras en el frontal de los vehículos para la prevención e investigación de accidentes que captaría la vía pública por la que circula el autobús, indicando que reducirían al máximo el ángulo de captación.

En lo que respecta a la legitimación para el tratamiento de datos descritos procede analizar si el tratamiento se podría encontrar amparado por el **interés legítimo** regulado en el artículo 7.f) de la Directiva 95/46/CE.

En cuanto a esta legitimación amparada en el artículo 7.f) de la Directiva 95/46/CE debe traerse a colación lo ya indicado por esta Agencia en su informe de 12 de marzo de 2012:



“El marco normativo en materia de protección de datos se ha visto sensiblemente afectado por la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, por la que se resuelven las cuestiones prejudiciales planteadas por el Tribunal Supremo en el seno de los recursos interpuestos por diversas asociaciones, entre ellas la propia consultante, contra el Reglamento de desarrollo de la Ley Orgánica 15/1999. A su vez, el marco se ve igualmente afectado por las Sentencias dictadas por el Tribunal Supremo en fecha 8 de febrero de 2012, por las que se resuelven los mencionados recursos.

La Sentencia del Tribunal de Justicia ha declarado expresamente el efecto directo del artículo 7 f) de la Directiva 95/46/CE, según el cual “Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva”. Por ello, dicho precepto deberá ser tomado directamente en cuenta en la aplicación de la normativa de protección de datos de carácter personal por los Estados Miembros, y en consecuencia por esta Agencia Española de Protección de Datos, dado que como señala el Tribunal Supremo en su sentencia de 8 de febrero de 2012 “produce efectos jurídicos inmediatos sin necesidad de normas nacionales para su aplicación, y que por ello puede hacerse valer ante las autoridades administrativas y judiciales cuando se observe su trasgresión”.

Tal y como recuerda la Sentencia del Tribunal de Justicia de la Unión Europea en su apartado 38, el artículo 7 f) de la Directiva “establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado” y, en relación con la citada ponderación, el apartado 40 recuerda que la misma “dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado”.



Por este motivo, la sentencia señala en su apartado 46 que los Estados miembros, a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46, deberán “procurar basarse en una interpretación de ésta que les permita garantizar un justo equilibrio entre los distintos derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión, por lo, conforme a su apartado 47 que “nada se opone a que, en ejercicio del margen de apreciación que les confiere el artículo 5 de la Directiva 95/46, los Estados miembros establezcan los principios que deben regir dicha ponderación”.

Por tanto, para determinar si procedería la aplicación del citado precepto habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis existe un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado o si, por el contrario, dichos derechos fundamentales o intereses de los interesados a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable pretende fundamentar el tratamiento de los datos de carácter personal.

En el presente caso, el interés legítimo alegado parece referirse especialmente al derecho fundamental a la tutela judicial efectiva (art. 24 CE), en la medida en que las imágenes grabadas únicamente se utilizarán para la obtención de pruebas con la finalidad de determinar las responsabilidades asociadas a la producción de un evento, o como señalan, *“la prevención e investigación de accidentes”*

En este sentido, alcance del derecho a la tutela judicial en relación con la prueba ha sido abordado, entre otras, en la STC 212/2013, de 16 de diciembre, en la que se hace referencia, citando la STC 88/2014, de 28 de mayo a *“las íntimas relaciones del derecho a la prueba con otros derechos garantizados en el art. 24 CE. Concretamente, en nuestra doctrina constitucional hemos hecho hincapié en la conexión de este específico derecho constitucional con el derecho a la tutela judicial efectiva (art. 24.1 CE), cuyo alcance incluye las cuestiones relativas a la prueba (SSTC 89/1986, de 1 de julio, FJ 2; 50/1988, de 22 de marzo, FJ 3; 110/1995, de 4 de julio, FJ 4; 189/1996, de 25 de noviembre, FJ 3; y 221/1998, de 24 de noviembre, FJ 3), y con el derecho de defensa (art. 24.2 CE), del que es inseparable (SSTC 131/1995, de 11 de*



septiembre, FJ 2; 1/1996, de 15 de enero, FJ 2; y 26/2000, de 31 de enero, FJ 2)” (STC 19/2001, de 29 de enero, FJ 4; y, en el mismo sentido, STC 133/2003, de 30 de junio, FJ 3)». En las reseñadas SSTC 19/2001 y 133/2003 el Tribunal Constitucional apuntaba que “ha sido justamente esta inescindible conexión (con los otros derechos fundamentales mencionados, en particular el derecho a obtener una tutela judicial efectiva), la que ha permitido afirmar que el contenido esencial del derecho a utilizar los medios de prueba pertinentes se integra por el poder jurídico que se reconoce a quien interviene como litigante en un proceso de provocar la actividad procesal necesaria para lograr la convicción del órgano judicial sobre la existencia o inexistencia de los hechos relevantes para la decisión del conflicto objeto del proceso (por todas, STC 37/2000, de 14 de febrero, FJ 3)”.

La relación entre los derechos a la protección de datos personales y a la tutela judicial ha sido, asimismo, analizada en el Informe de 30 de diciembre de 2011, en el que se indica lo siguiente:

“En este punto, debe recordarse que esta Agencia ya ha tenido la ocasión de analizar la posible concurrencia en un determinado supuesto de tratamiento de datos de los derechos fundamentales a la protección de datos de carácter personal y a la tutela judicial efectiva del responsable del tratamiento. Así, se ha considerado por ejemplo que el tratamiento por un abogado de los datos de la parte contraria de su cliente encuentra su amparo en el reconocimiento a éste último por el artículo 24.1 de la Constitución de su derecho a la tutela judicial efectiva, lo que implica, según el apartado 2, la defensa letrada y el uso de los medios de prueba pertinentes para la defensa de su derecho. En este sentido, el informe de 21 de febrero de 2001 se señalaba lo siguiente:

“En este caso, como se dijo, el tratamiento por los abogados y procuradores de los datos referidos a la contraparte de sus clientes en los litigios en que aquéllos ejerzan la postulación procesal trae su causa, directamente, del derecho de todos los ciudadanos a la asistencia letrada, consagrado por el artículo 24.2 del Texto Constitucional.

En efecto, la exigibilidad del consentimiento del oponente para el tratamiento de sus datos por el abogado o procurador supondría dejar a disposición de aquél el almacenamiento de la información necesaria para que su cliente pueda ejercer, en plenitud, su derecho a la tutela judicial efectiva. Así, la falta de estos datos puede implicar, lógicamente, una merma en la

posibilidad de aportación por el interesado de “los medios de prueba pertinentes para su defensa”, vulnerándose otra de las garantías derivadas del citado derecho a la tutela efectiva y coartándose la posibilidad de obtener el pleno desenvolvimiento de este derecho.

Por todo ello, si bien ninguna disposición con rango de Ley establece expresamente la posibilidad del tratamiento por abogados y procuradores de los datos referidos al oponente de su cliente en el seno de un determinado proceso judicial, es evidente que dicha posibilidad trae causa directa de una norma de rango constitucional, reguladora además de uno de los derechos fundamentales y libertades públicas consagrados por la Constitución, y desarrollado por las leyes reguladoras de cada uno de los Órdenes Jurisdiccionales, en los preceptos referidos a la representación y defensa de las partes.

Por todo ello, existe, desde nuestro punto de vista, una habilitación legal para el tratamiento de los datos, que trae su cobertura del propio artículo 24 de la Constitución y sus normas de desarrollo.”

El informe concluye afirmando que, en principio, sería posible entender que el tratamiento y la cesión de datos podrían entenderse amparadas y legitimadas en los artículos 6.11 y 11.2.a) de la LOPD, en conexión con el artículo 24 de la Constitución, siempre que se cumplan las garantías aportadas.

El citado informe analiza también la conexión entre esta última conclusión y la legitimación amparada en el artículo 7.f) de la Directiva 95/46/CE, reiterando al necesidad de ponderar si el derecho a la tutela judicial efectiva y a la defensa alegados por la consultante prevalecen o no sobre el derecho a la protección de los datos personales.

Partiendo de estas premisas, procede, por tanto, llevar a cabo esta ponderación atendiendo a las circunstancias específicas del caso al que se refiere la consulta. Para ello, deberán tenerse en cuenta, adicionalmente, las previsiones de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de seguridad en lugares públicos.

La norma citada atribuye a las Fuerzas y Cuerpos de Seguridad la competencia exclusiva para la instalación de videocámaras fijas o móviles en

lugares públicos, circunstancia que concurre en la presente consulta, al menos, respecto de la captación de imágenes hacia el exterior del vehículo de transporte.

Así se ha reconocido en numerosas resoluciones de la Agencia, entre las que cabe citar la del E/00223/2013, en la que se afirma lo siguiente:

“Primeramente, respecto a la posible captación por parte de la entidad denunciada, a través de su sistema de videovigilancia, de imágenes de la vía pública, hay que señalar que para entender las especialidades derivadas del tratamiento de las imágenes en vía pública, es preciso conocer la regulación que sobre esta materia se contempla en el artículo 1 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos que establece: “La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública”.

Este precepto es preciso ponerlo en relación con lo dispuesto en el artículo 3 e) de la Ley Orgánica 15/1999, donde se prevé que: “Se regirán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

e) Los procedentes de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia”.

En virtud de todo lo expuesto, podemos destacar que la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, señalándose en su artículo 2.2, en lo que hace mención a su ámbito de aplicación que “Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizados de los Datos de Carácter Personal.”



No obstante, la misma resolución admite una legitimación limitada para la captación de imágenes en la vía pública siempre que se garantice el cumplimiento del principio de proporcionalidad regulado en el artículo 4.1 y 2 de la LOPD, que establece lo siguiente: *“1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”*.

En relación con la captación de imágenes con fines de videovigilancia, dicho principio se refleja en el artículo 4 de la Instrucción 1/2006, de 8 de noviembre, con el siguiente tenor literal: *“Principios de calidad, proporcionalidad y finalidad del tratamiento. 1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras. 2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal. 3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida”*.

Si bien el artículo transcrito está relacionado con una finalidad, como es la videovigilancia por razones de seguridad, distinta de la que es objeto de la consulta; también en este caso será preciso garantizar específicamente el cumplimiento del principio de proporcionalidad.

A los efectos de ponderar la prevalencia o no del interés legítimo alegado, y, en particular, la garantía del principio de proporcionalidad, han de valorarse las garantías propuestas para la captación y uso posterior de las

imágenes. Ahora bien, en el caso planteado no se proponen garantías de ningún tipo que pudieran ponderarse en los términos expuestos, por lo que sin limitaciones de ningún tipo debemos concluir que no cabe la implantación genérica, y sin límites, de la captación y grabación de imágenes.

Por último, podemos referirnos al informe de esta Agencia de 13 de abril de 2015 en el que se planteaba la utilización de cámaras en el frontal de vehículos con la finalidad de obtener pruebas para el caso en que se produjera un siniestro de tráfico. En dicho informe se concluyó favorablemente, considerando las específicas cautelas implantadas en el sistema en cuestión: como primer punto destacamos que el sistema de grabación únicamente se activaba en caso de producirse un evento concreto, lo que determinaría el posible acaecimiento de un siniestro, o bien la activación manual, como podría plantearse en la consulta que ahora nos ocupa al hablar de “*dar mayor seguridad a los trabajadores en su quehacer diario*”. Dicho informe se pronunciaba en los siguientes términos:

“La finalidad del tratamiento resulta legítima teniendo en cuenta su vinculación con el derecho a la tutela judicial, quedando excluido el uso de las imágenes para otros fines como el control laboral, así como la grabación del sonido en el interior del vehículo que quedará desactivado en su comercialización en España.

La vinculación al derecho a la tutela judicial se concreta en el hecho de que sólo se accederá a las imágenes cuando tenga lugar un evento que se identifica con accidentes o situaciones de peligro en el interior del vehículo, susceptible de generar responsabilidades en el ámbito jurisdiccional.

La comercialización del dispositivo queda limitada a medios de transporte públicos y privados concesionarios de licencias para el transporte de personas y/o mercancías quedando excluida su instalación en otro tipo de vehículos.

La captación de imágenes hacia el exterior queda limitado al frontal del vehículo y, hacia el interior, excluye la captación de la imagen del conductor.

Adicionalmente, las grabaciones efectuadas se cancelan progresivamente pudiendo recuperarse sólo en el caso de producirse un evento. En tal caso la recuperación de las grabaciones queda limitada a un

periodo de tiempo máximo de 20 segundos anteriores y posteriores al momento del evento.

El acceso a los videos grabados se restringe a personas específicamente autorizadas con credenciales específicas y cuentas dedicadas.

En el tratamiento de las imágenes después de producirse el evento, se difuminarán las de las personas u otros datos como matrículas que no estén involucradas en el mismo.

El conjunto de restricciones que se han descrito permite minimizar el tratamiento de los datos personales quedando limitado a los datos adecuados, pertinentes y no excesivos en relación con la finalidad para la que se obtuvieron.

En cuanto a la conservación de los datos, el dispositivo permite un registro máximo de 300 eventos cancelándose automáticamente por orden de antigüedad una vez que se haya alcanzado dicho límite. No obstante, se prevé un plazo temporal de conservación de las imágenes por un periodo máximo de tres años, que se justifica por ser el plazo de prescripción de las infracciones muy graves reguladas en la LOPD.

Alternativamente se contempla la posibilidad de que dicho plazo sea el de un año previsto en el artículo 1968 del Código civil para la prescripción de acciones.

En este punto la decisión del Garante a que antes se hizo referencia vincula la conservación de las imágenes con los plazos de prescripción de las acciones legales frente a la producción de los daños causados como consecuencia del evento; criterio que cumple con mayor rigor el principio de proporcionalidad respecto de la finalidad declarada de posibilitar la obtención de pruebas en el ejercicio del derecho a la tutela judicial. Lo que no obsta a la conservación por un plazo superior de aquellas imágenes directamente vinculadas a una investigación policial o un procedimiento ya iniciados.

Las medidas de seguridad propuestas para el tratamiento de los datos son los que el artículo 81 y concordantes del RLOP califica como de nivel medio, criterio que puede vincularse al hecho de que, en ocasiones, las

imágenes estarán relacionadas con la comisión de infracciones administrativas o penales.

Respecto de la transparencia en el tratamiento de los datos, es decir, de la información que ha de facilitarse a los interesados, la consulta describe un abanico de opciones que se complementan entre sí, e incluyen un cartel visible en el interior del vehículo, la incorporación de cláusulas informativas en la documentación dirigida a los pasajeros y en la página web del responsable del tratamiento o, en su caso, de sus perfiles sociales. A los que se añade la realización de una campaña informativa por parte de los responsables del tratamiento sobre el uso y las funcionalidades del dispositivo previa al tratamiento de los datos a través de sus servicios de atención al cliente. El conjunto de opciones propuestas permitirían, por tanto, garantizar que los interesados puedan obtener la información requerida por el artículo 5 de la LOPD. En particular, la campaña informativa a través de los servicios de atención al cliente coincide con la recomendación que en idéntico sentido incluyo la decisión del Garante antes citada.

No obstante, se excluye la información sobre las cesiones a jueces y a la policía estando esta última excluida entre las previstas en el artículo 11.2. d) de la LOPD, por lo que debería completarse la información.

Sobre la información para el tratamiento de datos en el exterior del vehículo no se indica una fórmula específica, si bien cabría admitir un procedimiento simplificado análogo al contemplado en la Instrucción 1/2006, de 8 de noviembre, consistente en un pictograma o dibujo de fácil comprensión sobre la finalidad del tratamiento y el responsable ante el que pueden ejercitarse los derechos ARCO.

Dicha información debería completarse implantando procedimientos para poner a disposición de los interesados el resto de los extremos recogidos en el artículo 5 de la LOPD.

Teniendo en cuenta cuanto se acaba de indicar, aplicada la regla de ponderación exigida por el TJUE al objeto de la consulta, cabe concluir que los tratamientos de datos, siempre que cumplan todas las garantías que se han descrito, se encuentran amparadas en el artículo 7.f) de la Directiva 95/46/CE en conexión con el artículo 24 de la Constitución”.